

Inventario de redes y protocolos activos

El presente es un listado de aquellos protocolos utilizados en la operatoria general del servicio de pagos. Se incluye datos relacionados, puertos activos, protocolo utilizado, aplicación que lo accede, justificación de negocio y características de seguridad implementadas para la mitigación de riesgos.

Tabla de Contenidos

- [Tabla de Contenidos](#)
- [Inventario de activos cloud en uso \(AWS\)](#)
- [Inventario de redes confiables y no confiables](#)
- [Inventario y Controles de protocolos UDP/TCP](#)
 - [Puerto 443 \(https\)](#)
 - [Puerto 5044 \(filebeat\)](#)
 - [Puerto 22 \(ssh\)](#)
 - [Puerto 27017 \(mongodb\)](#)
 - [Puertos 514, 1514, 1515, 1516 \(Wazuh\)](#)
- [Control de Cambios](#)

Inventario de activos cloud en uso (AWS)

Activo	Nombre	Descripción
VPC	Virtual Private Cloud	Entorno virtual de redes. Define redes y permite la segmentación en subredes.
SG	Security Group	Firewall virtual para controlar tráfico entrante y saliente.
RT	Route Tables	Tablas de enrutamiento.
IGW	Internet Gateway	Gateway de acceso a internet para subredes públicas.
NGW	NAT Gateway	Gateway que realiza NAT para redes privadas.
EIP	Elastic IP	Provisión de IPs públicas fijas para subredes públicas.
R53	Route 53	Provisión de servicio DNS privado.
Peering Connection	Peering Connection	Conexión punto-a-punto entre VPCs.

Inventario de redes confiables y no confiables

La siguiente tabla incluye todas las redes y subredes confiables y no confiables relacionadas a operaciones de pago con tarjeta de crédito, control y auditoría.

Nombre	AWS VPC ID	Bloque CIDR	Descripción	Alcance PCI DSS	Nivel de confianza	Sensibilidad
vpc-pci-transit	vpc-0c3296ab1b b4aefb1	10.1.0.0 /16	Red destinada a los accesos (transito) públicos, por ejemplo, sesionamiento SSH a instancia bastión.	EN ALCANCE	CONFIABLE	MEDIA
vpc-pci-internal	vpc-0c6c7021bb 5a4b657	10.10.0.0 /16	Contiene los sistemas que almacenan, procesan y transmiten datos de tarjetas: servidores de aplicación, bases de datos, etc.	EN ALCANCE	CONFIABLE	ALTA
paypertic-prod-vpc	vpc-a34475cb	10.20.0.0 /16	Red específica para el procesador principal de pagos, recibe y envía datos de pagos y pagadores.	EN ALCANCE	CONFIABLE	ALTA
peypertic-dev-vpc	vpc-006a387b88 3d2a2b9	10.120.0.0 /16	Entorno para desarrollo y pruebas. No se utilizan datos de tarjetas del entorno productivo.	FUERA DE ALCANCE	CONFIABLE	BAJA
Internet	N/A	0.0.0.0/0	Red pública global	FUERA DE ALCANCE	NO CONFIABLE	

Inventario y Controles de protocolos UDP/TCP

Puerto 443 (https)

- **Protocolo:** TCP

- **Servicio relacionado:** nginx
- **Justificación de uso:** Se utiliza para el acceso de las distintas partes del circuito de pagos para consulta/inserción de tokens de PAN en el entorno compliant.
- **Características de seguridad:**
 - El tráfico es cifrado mediante el uso de protocolos robustos (TLS 1.2 o superior, donde es posible).
 - Se utilizan certificados digitales válidos, emitidos por una Autoridad Certificante (CA) reconocida.
 - No se permiten los conjuntos de cifrado débiles.

Puerto 5044 (filebeat)

- **Protocolo:** TCP
- **Servicios relacionados:**
 - AWS Cloudwatch
 - Filebeat
- **Justificación de uso:** Recolección de logs para monitoreo de seguridad y auditoría.
- **Características de seguridad:**
 - La comunicación entre los agentes filebeat y el servicio de AWS Cloudwatch está cifrada mediante TLS para proteger la integridad y confidencialidad de los logs en tránsito.
 - El acceso a este puerto está restringido a nivel de red para permitir conexiones únicamente desde las instancias autorizadas.

Puerto 22 (ssh)

- **Protocolo:** TCP
- **Servicio relacionado:** ssh
- **Justificación de uso:** Necesario para el ingreso a la consola de administración de las instancias privadas. Este acceso es solo posible por personal de operaciones autorizado.
- **Características de seguridad:**
 - Se deshabilita la autenticación por contraseñas. El acceso se da solamente utilizando pares de llaves criptográficas.
 - Se restringe el acceso a este puerto mediante el uso de firewall (security groups) para permitir conexiones solo desde las direcciones IP de administración ya definidas (bastión host).
 - Se utilizan algoritmos de cifrado, intercambio de claves y MACs robustos.

Puerto 27017 (mongodb)

- **Protocolo:** TCP
- **Servicio relacionado:** MongoDB
- **Justificación de uso:** Comunicación de la aplicación con la base de datos documental.
- **Características de seguridad:**
 - El puerto no se expone en redes públicas, solo es posible accederse desde la capa de aplicación (tier 2).
 - La comunicación se encuentra cifrada.
 - El acceso a bases de datos requiere autenticación.

Puertos 514, 1514, 1515, 1516 (Wazuh)

- **Protocolo:** UDP/TCP (514), TCP (1514, 1515, 1516)
- **Servicio relacionado:** IDS (Wazuh)
- **Justificación de uso:**
 - 514: Recolector de syslog para Wazuh.
 - 1514, 1515: Conexión del agente recolector.
 - 1516: Comunicación interna del clúster del daemon Wazuh.
- **Características de seguridad:**
 - Estos puertos son únicamente para la comunicación interna de la herramienta de seguridad (IDS).
 - El acceso está estrictamente restringido a nivel de red (firewall/SG) para permitir la comunicación entre agentes Wazuh y servidores del clúster.
 - Cualquier intento de conexión externo a este perímetro definido es denegado y alertado.

Control de Cambios

Version	Published	Changed By	Comment
CURRENT (v. 2)	Oct 11, 2025 22:05	Maximiliano Nicoletti	
v. 1	Oct 09, 2025 16:31	Maximiliano Nicoletti	